



یک الگوریتم نهان نگاری مقاوم بر اساس پرش فرکانسی

سمیه مهدوی جعفری^۱، سعید رضا صید نژاد^۲، سعید سریزدی^۳

دانشگاه شهید باهنر کرمان^۱

s.mahdavi.j@gmail.com

کرمان، دانشگاه شهید باهنر کرمان، گروه مهندسی برق^{۲ و ۳}

elecdept@uk.ac.ir

چکیده

در این مقاله یک الگوریتم نهان نگاری صوتی جدید بر مبنای ایده پرش فرکانسی ارائه شده است. دو مجموعه جداگانه از فرکانس‌های متفاوت برای انتقال بیت "۰" و "۱" بکار می‌رود. این فرکانس‌ها به گونه‌ای انتخاب شده‌اند که واترمارک تزریقی ضمن نامحسوس بودن، در برابر حملات نیز مقاومت نماید. برای نهفتن هر بیت از پیام باینری در یک قسمت از سیگنال صوت، یک زوج فرکانسی بصورت تصادفی از مجموعه فرکانس‌های داده شده، انتخاب می‌شود. بر اساس بیت پیام و محتوای فرکانسی آن قسمت از سیگنال صوت، یک فرکانس از جفت فرکانسی بدست آمده انتخاب می‌شود. یک حامل سینوسی در این فرکانس به عنوان سیگنال واترمارک تولید می‌شود. دامنه این حامل سینوسی توسط فیلترهای باند بحرانی مدل کننده سیستم شنیداری انسان (HAS) شکل داده می‌شود. خواص مینتی بر محتوای الگوریتم پیشنهادی، سبب ارائه ظرفیت بالا، مقاومت بالا و کیفیت بالا بطور همزمان گردیده است. نتایج آزمایشات و شبیه‌سازی انجام شده، نشان دهنده مقاومت بالای الگوریتم پیشنهادی در برابر تمامی حملات متداول برای انواع کلیپ‌های صوتی می باشد.

واژه‌های کلیدی

نهان نگاری صوتی، سیستم شنیداری انسان، فیلترهای باند بحرانی، پرش فرکانسی.

۱- مقدمه !

باشند. ولی مقاومت آنها در سیگنالهایی که تعداد مؤلفه‌های حوزه تبدیلشان بسیار کم می باشد رضایت بخش نیست [1]. علاوه بر این، این الگوریتم‌ها نسبت به الگوریتم‌های حوزه زمان پیچیده تر و زمانبرتر می باشند.

روشهای حوزه زمان عموماً از دو استراتژی استفاده می کنند: ۱- دستکاری کردن نمونه‌های سیگنال به منظور نهفتن بیت واترمارک (روش رمزگذاری بیت کم ارزش^[2])، روش چندی سازی^[3] و غیره^[4,5] ۲- اضافه کردن نویز نا محسوس (سیگنال واترمارک) که پیام را حمل می کند به سیگنال میزبان (روش‌های طیف گسترده^[6]، پنهان کردن تأخیر^[7,8] و غیره

نهان نگاری صوتی فرآیند نهفتن اطلاعات اضافی در سیگنال میزبان به منظور اثبات حق مالکیت می باشد. واتر مارک نهان شده بایستی دارای شرایط زیرباشد:

نامحسوس بودن

غیرقابل آشکارشدن برای افراد غیر مجاز به منظور ممانعت از حذف شدن

مقاوم بودن در برابر کلیه حملات پردازش سیگنال

قابل آشکارشدن برای اثبات حق مالکیت

الگوریتم‌های نهان نگاری صوتی عموماً به دو گروه حوزه زمان و حوزه تبدیل تقسیم بندی می شوند. الگوریتم‌های حوزه تبدیل نسبت به الگوریتم‌های حوزه زمان در مقابل حملات مقاومتر می

¹ LSB Coding

² Quantization

³ Spread Spectrum

نمونه از سیگنال صوت سبب کاهش محسوس کیفیت سیگنال صوت می گردد، لذا با انتخاب ۱۰۲۴ به عنوان طول پنجره، مقاومت الگوریتم در برابر برش تضمین می گردد. البته پنجره های بزرگتر اگر چه اطمینان بخش خواهند بود، ولی منجر به کاهش نرخ نهانگی و ظرفیت الگوریتم می شوند. حال آنکه انتخاب ۱۰۲۴ به عنوان کمترین طول قابل قبول، نرخ نهانگی قابل قبولی را ارائه می دهد.

برای نهفتن بیت های پیام از حامل های سینوسی با فرکانسهای متفاوت استفاده می شود. در واقع فرکانس حامل مشخص کننده ماهیت بیت پیام ارسالی می باشد. برای تحقق این منظور از ایده پرش فرکانسی در سیستم های مخابراتی طیف گسترده استفاده می شود. بدین منظور یک حامل به صورت تصادفی انتخاب و به عنوان واترمارک با پنجره جمع می شود. مقاومت و شفافیت الگوریتم پیشنهادی به شدت وابسته به فرکانس حامل، روش پرش و نحوه شکل دهی دامنه حامل که بعداً توضیح داده خواهد شد، می باشد. فرآیند نهانگی الگوریتم پیشنهادی به چهار قسمت تقسیم می شود:

انتخاب اولیه فرکانسها

چیدمان نهایی فرکانسها

شکل دهی نویز

نهفتن واتر مارک

در ادامه به توضیح هر یک از این مراحل می پردازیم.

۲-۱. انتخاب اولیه فرکانسها

اولین گام تعریف دو مجموعه جداگانه از فرکانسها به نام مجموعه "۰" و مجموعه "۱" می باشد. طول این دو مجموعه مساوی و برابر L می باشد. اعضای مجموعه "۰" برای نهفتن بیت پیام "۰" و اعضای مجموعه "۱" برای نهفتن بیت پیام "۱" مورد استفاده قرار می گیرند. هر عضو از مجموعه "۱" با عضو نظیرش در مجموعه "۰" یک جفت فرکانس (f_{0m}, f_{1m}) نامیده می شوند.

$$\text{Set}_0: \{f_{01}, \dots, f_{0L}\}$$

$$\text{Set}_1: \{f_{11}, \dots, f_{1L}\} \quad (1)$$

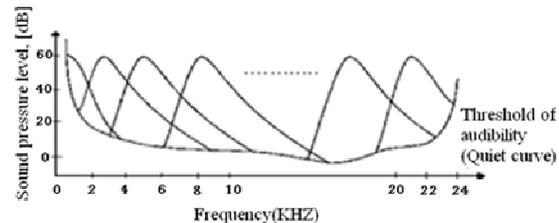
که در آن L تعداد فرکانس های انتخابی و طول مجموعه می باشد. تعریف فرکانسهای "۰" (اعضای مجموعه "۰") و فرکانسهای "۱" (اعضای مجموعه "۱") با رعایت چهار شرط صورت می پذیرد:

۱. بین فرکانسهای "۰" (اعضای مجموعه "۰") و بین فرکانسهای "۱" (اعضای مجموعه "۱") بایستی فاصله کافی وجود داشته باشد.

۲. هر فرکانس بایستی تنها به فرکانس مرکزی یکی از فیلترهای بحرانی کمترین فاصله را داشته باشد. به عبارت دیگر هر کدام از این فرکانسها بر اساس فاصله اش به فرکانس مرکزی فیلتر های بحرانی، بایستی تنها

[1],[9,11]) تقریباً تمامی الگوریتمهای حوزه زمان از خواص سیستم شنیداری انسان [12] برای نامحسوس نمودن نویز تریقی استفاده می کنند.

سیستم شنیداری انسان به عنوان یک سیستم آنالیز کننده فرکانسی توسط ۲۵ فیلتر میانگذر (اصطلاحاً باندهای بحرانی^۱) مدل می شود که رنج فرکانسی ۱۰ هرتز تا ۲۰ کیلو هرتز را می پوشانند (شکل ۱). دامنه این فیلترها به یک منحنی که منحنی حد آستانه سکوت نام دارد محدود می شود [12].



شکل ۱. فیلترهای بحرانی مدل کننده HAS

در بین تمامی روشهای شکل دهنده نویز که پیش از این به آن اشاره شد، فقط [10] از حامل سینوسی برای نهفتن بیت پیام استفاده می کند. [10] از فرکانس متوسط لحظه ای هر قسمت از سیگنال صوت به عنوان فرکانس حامل و برای نهفتن بیت پیام از مدولاسیون دامنه استفاده کرده است. این الگوریتم ضمن عدم مقاومت در برابر حمله برش و عبور از فیلتر، در شرایط ناهمزمانی گیرنده و فرستنده دچار مشکل خواهد شد.

در این مقاله ما یک روش شکل دهنده نویز جدید در حوزه زمان بر اساس تئوری پرش فرکانسی در تکنیکهای گسترده طیف [13]، ارائه می دهیم. بر خلاف اکثر الگوریتمها که از دنباله های شبه نویز (فرمت مدولاسیون دامنه) برای نهفتن بیت پیام استفاده می کنند [10]، ما از حامل های سینوسی تصادفی (فرمت مدولاسیون فرکانس) به این منظور استفاده می کنیم. برای نامحسوس نمودن واترمارک از توزیع انرژی هر قسمت از سیگنال در فیلترهای باند بحرانی سیستم شنیداری انسان، استفاده می شود. این الگوریتم به همزمانی گیرنده و فرستنده وابسته نبوده و در برابر کلیه حملات بویژه برش مقاوم می باشد.

۲- نهفتن واترمارک

ابتدا سیگنال صوت به بازه هایی با طول مساوی تقسیم می شود. اصطلاحاً این بازه ها پنجره نامیده می شوند. در هر پنجره از سیگنال صوت یک بیت از پیام باینری نهفته می شود. طول پنجره به گونه ای انتخاب گردیده است که پیام نهان شده در برابر حمله برش مقاوم باشد. با توجه به اینکه حذف بیش از ۵۰۰ الی ۶۰۰

¹ Human Auditory System (HAS)

² Critical Bands

صورت پیش فرض قرار بر نهان ساختن f_0 باشد، اما E_0 کمتر از E_1 باشد، آنگاه فرکانس f_0 با f_1 جا به جا می شوند. بر عکس اگر بیت پیام "۱" باشد و به صورت پیش فرض قرار بر نهان ساختن f_1 باشد، اما E_1 کمتر از E_0 باشد، آنگاه فرکانس f_1 با f_0 جا به جا می شوند. لذا برای نهفتن بیت i ام در پنجره i ام فرکانس انتخابی به شرح زیر خواهد بود:

(۲)

$$f_i = \begin{cases} f_0 & \text{if } b=0 \text{ and } E_0 > E_1 \text{ or if } b=1 \text{ and } E_1 < E_0 \\ f_1 & \text{if } b=1 \text{ and } E_1 > E_0 \text{ or if } b=0 \text{ and } E_0 < E_1 \end{cases}$$

که در آن b نشاندهنده i امین بیت پیام می باشد. برای مشخص نمودن تمام جابه جایی های فرکانسها برای گیرنده مجاز، یک کلید رمز ۲ تعریف می شود که در حالتی که هیچ جا به جایی صورت نپذیرد "۰" و در صورت بروز جا به جایی "۱" خواهد بود.

۲-۳- فرآیند شکل دهی!

در مرحله قبل مشخص می شود کدام حامل در پنجره بایستی نهفته شود. دامنه حامل در ابتدا برابر واحد می باشد. اما دامنه این حامل بایستی به شیوه مناسبی بر اساس خواص HAS شکل داده شود تا ناشنیدنی گردد (رابطه ۳).

$$w_i(t) = \gamma \times (\alpha \times |h_i(t)| + \beta \times |g_i(t)|) \times \cos(2\pi f_i t) \quad (3)$$

که در آن:

$$w_i(t): \text{سیگنال واترمارک } i \text{ امین پنجره}$$

$$g_i(t): s_i(t) - h_i(t)$$

$$s_i(t): \text{سیگنال صوت ابتدایی در } i \text{ امین پنجره}$$

$$h_i(t): \text{سیگنال صوت فیلتر شده در } i \text{ امین پنجره}$$

$$\alpha, \beta, \gamma: \text{اعداد ثابت}$$

می باشد. برای ساختن $h_i(t)$ ، سیگنال ابتدایی در i امین پنجره $(s_i(t))$ ، از فیلتر بحرانی نظیر فرکانس انتخاب شده در رابطه (۲) عبور می کند. $h_i(t)$ به عنوان سیگنال غالب در نظر گرفته می شود و با ضریب α تضعیف می گردد. تفاضل سیگنال ابتدایی و سیگنال خروجی فیلتر نیز به عنوان یک پارامتر دیگر در نظر گرفته می شود. این سیگنال به عنوان نویز زمینه در نظر گرفته می شود و با ضریب β تضعیف می گردد. سیگنالهای حاصله با هم جمع می گردند. سیگنال منتج با پارامتر دیگری به نام γ تضعیف می گردد و نتیجه در حامل انتخاب شده ضرب می گردد تا سیگنال واتر مارک را ایجاد کند. پارامترهای α و β جهت برقراری توازن بین سیگنال غالب و نویز زمینه به کار می روند. در واقع توازن بین مقدار α و معین کننده میزان نرخ بیت خطا می باشد. γ برای زیر آستانه سکوت نگه داشتن نویز تزریقی به کار می رود و کنترل نامحسوس نمودن نویز تزریقی را برعهده دارد.

به یکی از آنها تعلق داشته باشد.

۳. فاصله کافی بین فرکانسهای هر جفت فرکانسی بایستی در نظر گرفته شود.

۴. عموماً سیگنالهای صوت فرکانسهای بسیار پایین نمی باشند. لذا تمامی فرکانسها بالای حد ۲۰۰ هرتز انتخاب می شوند. همچنین تمامی فرکانسها زیر حد ۴ کیلوهرتز انتخاب می شوند. این فرکانس قطع فیلتر پایین گذاری است که اکثراً در حملات مورد استفاده قرار می گیرد.

مجموعه فرکانسهای پیش فرض به کار برده شده برای نهفتن

بیت "۰" و بیت "۱" به شرح زیر می باشند:

$$set0 = [225 \ 275 \ 325 \ 375 \ 425 \ 475 \ 545 \ 595 \ 675 \ 725 \ 815 \ 865 \ 975 \ 1025 \ 1145];$$

$$set1 = [1195 \ 1345 \ 1395 \ 1575 \ 1625 \ 1825 \ 1875 \ 2125 \ 2175 \ 2475 \ 2525 \ 2875 \ 2925 \ 3375 \ 3425];$$

۲-۲- چیدمان نهایی فرکانسها!

تغییر چیدمان پیش فرض فرکانسها در دو مرحله صورت می پذیرد:

۱. ابتدا یک تولید کننده اعداد تصادفی برای ساختن یک دنباله تصادفی از ۱ تا L مورد استفاده قرار می گیرد. نقطه شروع تولید کننده اعداد تصادفی یک کلید رمز (دنباله PN) می باشد (کلید رمز ۱). بنابراین برای نهفتن i امین بیت پیام، i امین عدد تولید شده، مشخص می کند که کدام جفت از فرکانسهای تولیدی (L تا ۱) مورد استفاده قرار گیرند.

۲. پس از انتخاب یک جفت فرکانسی در مرحله قبل (f_{0m}, f_{1m}) ، از بین دو فرکانس موجود در جفت فرکانسی، یک فرکانس مناسب برای نهفتن بیت پیام مورد استفاده قرار می گیرد. یکی از ویژگی های بارز الگوریتم پیشنهادی وفقی بودن آن است. به این مفهوم که در این الگوریتم سعی بر آن است که فرکانس انتخابی هر پنجره با محتویات فرکانسی آن پنجره نزدیکی داشته باشد. جهت تحقق این هدف، از مدل سیستم شنیداری انسان استفاده می شود. از آنجا که هر کدام از فرکانسهای انتخابی به باندهای بحرانی جداگانه ای تعلق دارند، لذا انرژی پنجره در باندهای بحرانی نظیر فرکانسهای انتخاب شده، محاسبه می شود (E_0, E_1) . برای این کار، فیلترهای مدل کننده HAS با ۲۵ فیلتر میانگذر FIR با مرتبه ۱۰۰ که باند گذر هر کدام بر یکی از باندهای بحرانی منطبق می باشد، شبیه سازی شده اند. حال فرض کنید که E_0 انرژی m امین فیلتر بحرانی متناظر با f_0 و E_1 انرژی n امین فیلتر بحرانی متناظر با f_1 باشد. اگر بیت پیام "۰" باشد و به

جاز^۷، پیانو^۸، کلاسیک^۹، محلی^{۱۰}، نی (تک نوازی)^{۱۱}، سنتور (تک نوازی)، صحبت^{۱۲} (زن و مرد) و صوت با بازه های طولانی سکوت (از هر نوع ۲ موسیقی) تست کردیم. اگرچه مقالات پیشین هر یک تعداد اندکی از این اصوات را مورد آزمایش قرار دادند، ولی ما در این مقاله مجموعه ای از کلیه این اصوات گردآوری کرده و مورد آزمایش قرار دادیم. جهت تطابق با کیفیت اصوات موجود در CD های رایج، در این کلیهها فرکانس نمونه برداری ۴۴/۱ کیلو هرتز و هر نمونه با ۱۶ بیت نمایش داده می شوند.

۴-۱- تست شنیداری!

ارزیابی کیفیت صوت حاوی واترمارک نسبت به سیگنال صوت ابتدایی با معیارهای عددی (به عنوان مثال بر اساس متوسط مجذور خطا یا نسبت سیگنال به نویز) مشکل است. زیرا بر اساس خواص گوش انسان حتی یک صوت با دامنه تغییر مقیاس یافته، ممکن است با وجود متوسط مجذور خطای بالا از کیفیت بسیار عالی برخوردار باشد [11]. بنابراین برای ارزیابی کیفیت صوت، (مطابق با آنچه که در سایر مقالات صورت گرفته است)، یک سری تست غیر رسمی با هدست انجام شده است. به این منظور کلیههای صوت ابتدایی و کلیههای صوت حاوی واترمارک دار به صورت تصادفی برای یک گروه ۱۰ نفره متشکل از افرادی با سنهای متنوع و جنس مختلف پخش گردید. هیچ تفاوتی بین اصوات پخش شده توسط افراد گروه تشخیص داده نشد و در تشخیص نوع صوت نیز صوت حاوی واترمارک بعضاً با صوت اصلی اشتباه گرفته شد. نتایج این آزمایشات گویای این مسئله است که همانطور که انتظار می رفت واتر مارک اضافه شده بر کیفیت سیگنال صوت اثر نمی گذارد. زیرا در شکل دهی کریپر تزریقی از مدل سیستم شنیداری انسان استفاده شده است.

۴-۲- تست مقاومت!

ضمن حفظ کیفیت سیگنال واترمارک دار شده، با اعمال یک سری از عملیات پردازش سیگنال، مقاومت این الگوریتمها مورد بررسی قرار گرفت. این حملات بر اساس آنچه که در سایر مقالات ذکر شده است، انتخاب گردیدند. برای مشخص شدن میزان مقاومت روشهای پیشنهادی حملات زیر به کار گرفته شدند.

۱. تغییر مقیاس محور زمان (T1)

ابتدا سیگنال واتر مارک دار شده تا حد ۴٪ در محور زمان

۴-۳- نهفتن واتر مارک!

بعد از ساختن حاملهای شکل داده شده، هر قسمت از سیگنال حاوی واتر مارک از جمع یک پنجره از سیگنال صوت ابتدایی با حامل نظیرش بدست می آید.

$$s_{w,i} = s_i + w_i \quad \text{for all } i \quad (4)$$

که در آن:

s_i : سیگنال میزبان در پنجره i ام،

w_i : حامل نظیر پنجره i ام،

$s_{w,i}$: سیگنال محتوی واتر مارک در پنجره i ام

می باشد.

۴-۳- آشکارسازی!

آشکار سازی بیت نهان شده مستلزم استخراج فرکانس حامل می باشد. آشکارسازی حامل هم از روشهای همزمان^۳ و هم از روشهای غیر همزمان^۴ امکانپذیر می باشد. اما از آنجا که روشهای همزمان در برابر حملاتی که همزمانی گیرنده و فرستنده را به هم می زند عملکرد مناسبی ندارند، ما مشابه آنچه که در تکنیکهای طیف گسترده ناشی از پرش فرکانسی استفاده می شود، از روشهای غیر همزمان (فیلترهای میانگذر) استفاده می کنیم.

فرآیند آشکارسازی شبیه فرآیند نهانگی می باشد. ابتدا سیگنال حاوی واترمارک به پنجره هایی تقسیم بندی می شود. سپس با اعمال کلیدرمز ۱ به تولید کننده اعداد تصادفی، دنباله تصادفی مورد استفاده در فرستنده بدست آمده و به مجموعه "۰" و مجموعه "۱" اعمال می شود تا ترتیب جفتهای فرکانسی مورد استفاده در گیرنده مشخص گردد. برای آشکار نمودن بیت i ام پیام، i امین قسمت از سیگنال از دو فیلتر میانگذر شبیه سازی شده نظیر جفت فرکانسی انتخاب شده، عبور می کند و E_1 و E_0 بدست می آید. حال با در نظر گرفتن بیت i ام کلید رمز ۲ و رابطه (۲) ماهیت بیت پیام آشکار می شود. در واقع کلید رمز ۱ مشخص می کند که کدام زوج فرکانسی استفاده شده است و کلید رمز ۲ بیت پیام را آشکار می کند.

۴-۴- نتیجه آزمایشهای انجام شده

برای بررسی عملکرد سیستم های پیشنهادی یک تست ناشنوائی و چند تست مقاومت صورت پذیرفت. ما الگوریتمهای پیشنهادی را با ۲۰ کلیپ موسیقی ۲۰ ثانیه ای مختلف از انواع پاپ^۵، راک^۶،

⁷ Jazz

⁸ Piano

⁹ Classic

¹⁰ Country

¹¹ Solo

¹² Speech

³ Coherent

⁴ Non-coherent

⁵ Pop

⁶ Rock

می باشد ارائه گردید. ایده پرش فرکانسی برای نهفتن بیت پیام بکار گرفته شد. این الگوریتم از خواص فیلترهای بحرانی سیستم شنیداری انسان به منظور انتخاب حامل و شکل دهی آن بهره برداری می کند. نتایج آزمایشات انجام شده نشان می دهد که الگوریتم پیشنهادی در برابر کلیه حملات پردازش سیگنال و برای انواع مختلف کلیپ های صوتی مقاوم بوده و نرخ نهانگی بالایی ارائه می دهد.

جدول ۱. تعداد بیت خطایی که در آشکارسازی پیام یک پیام ۳۲

بیتی در الگوریتم پرش فرکانسی رخ داده است

نوع موسیقی	T0	T1	T2	T3	T4	T5	T6	T7	T8	T9	
										1st	2nd
بیانوا	0	1	0	0	0	0	0	0	0	0	1
بیانوا ۲	0	0	0	0	1	0	0	0	0	0	1
راک ۱	0	0	0	0	1	0	1	1	0	0	1
راک ۲	0	0	0	0	0	0	0	0	0	0	0
جاز ۱	0	0	0	1	0	0	0	0	0	0	0
جاز ۲	0	0	0	0	0	0	0	0	0	0	0
محل ۱	1	1	1	1	1	1	12	4	1	1	4
محل ۲	1	3	1	2	1	1	10	3	1	1	1
کلاسیک ۱	0	0	0	0	0	0	0	0	0	0	0
کلاسیک ۲	0	0	0	0	0	0	0	0	0	0	0
پاپ ۱	0	0	0	1	0	0	1	1	0	0	0
پاپ ۲	0	0	0	0	0	0	1	1	0	0	2
بی (اتک نواری)	0	0	0	0	0	0	5	1	0	0	0
بی ۳ (اتک نواری)	0	0	0	0	2	0	1	1	0	0	1
سنسور (اتک نواری)	0	0	0	0	0	0	4	1	0	0	4
سنسور ۲ (اتک نواری)	0	0	0	0	1	0	3	2	0	0	1
صوت با سکوت ۱	0	0	0	0	1	0	2	2	0	0	0
صوت با سکوت ۲	0	0	0	0	1	0	2	3	1	0	5
صحبت (مرد)	0	0	0	0	0	0	1	0	0	0	1
صحبت (زن)	0	0	0	0	0	0	0	0	0	0	0

مراجع

- [1] A.N., Lemma, et. al., "A Temporal Domain Audio Watermarking Technique", IEEE Trans. Signal Proc., Vol. 51, No. 4, April 2003.
- [2] C.H. Yeh, et. al. "Digital watermarking through quasi m-arrays". Proc. IEEE Workshop on Signal Proc. Systems, Taipei, Taiwan, p 456-461, 1999.
- [3] H. J. Kim, et. al., "Audio Watermarking Techniques", J-s-Pan Ed. Chap 8, World, Scientific Pub. Co, 2004
- [4] M. F. Mansour, et. al., "Audio Watermarking by Time-Scale Modification", Proc. IEEE ICASSP Conf, pp. 1353-1356, 2001.
- [5] W-N Lie, et. al., "Robust and High-Quality Time-Domain Audio Watermarking Based on Low-Frequency Amplitude Modification", IEEE Trans. Multimedia, Vol. 8, pp. 46-59, Feb. 2006.

منبسط می گردد و سپس تا حد ۴٪ فشرده می گردد.

۲. تغییر نرخ نمونه برداری (T2)

نرخ نمونه برداری سیگنال واتر مارک داده ابتدا به ۴۴/۱ کیلو هرتز، بعد به ۳۲ کیلو هرتز و سپس به ۴۸ کیلو هرتز و نهایتاً به ۴۴/۱ کیلو هرتز تغییر می یابد.

۳. فیلتر پایین گذر (T3)

از یک فیلتر پایین گذر مرتبه ۴ باترورت با فرکانس قطع ۴ کیلو هرتز استفاده گردید.

۴. اضافه کردن نویز (T4)

نویزی با متوسط صفر و تابع چگالی توان گوسی به سیگنال حاوی واترمارک اضافه می شود.

۵. تغییر دامنه سیگنال (T5)

سیگنال واتر مارک دار با ضریب ۰/۱ تضعیف گردید.

۶. برش (T6)

چندین قسمت ۵۰۰ نمونه ای از محلهای مختلف سیگنال واترمارک دار حذف گردید و سپس آشکارسازی پیام نهفته شده مورد بررسی قرار گرفت.

۷. همزمانی (T7)

یک قسمت ۵۰۰ نمونه ای از ابتدای سیگنال حاوی واترمارک حذف گردید.

۸. اضافه کردن اکو (T8)

سیگنال ابتدایی با ۱۰۰ میلی ثانیه تأخیر به سیگنال حاوی واترمارک اضافه می شود.

۹. نهفتن چند واتر مارک (T9)

دو واتر مارک کاملاً مجزا در سیگنال صوت نهفته گردیدند و سپس نرخ آشکارسازی هر کدام مورد بررسی قرار گرفت.

جدول ۱ میزان بیت خطایی که در آشکارسازی پیام یک پیام ۳۲ بیتی پس از هر یک از این مراحل رخ داده است را نشان می دهد. در این جدول T0 میزان خطا در آشکارسازی طبیعی و بدون اعمال هیچ گونه حمله ای و T1, ..., T9 به ترتیب حملات ذکر شده را مشخص می کنند. همانطور که مشاهده می شود روش پیشنهادی به خوبی قادر به تحمل تمامی حملات می باشد. از طرفی اجرای این الگوریتم برای موسیقی نوع محلی با بیت خطا همراه می باشد. البته با نرخ نهانگی کمتر (با طول پنجره بیشتر) نتایج بهتری بدست می آید. این در حالی است که سایر الگوریتمها در برابر تعدادی از این حملات عملکرد خوبی ارائه نمی دهند. طبق پارامترهای انتخابی نرخ نهانگی الگوریتم پیشنهادی (ظرفیت) ۴۳ بیت بر ثانیه است که با تغییر پارامترهای انتخابی قابل افزایش می باشد.

۵- نتیجه گیری

یک روش جدید برای نهفتن واترمارک های دیجیتال در سیگنالهای صوتی که بویژه در برابر حملات برش و همزمانی مقاوم

- [10] Cheng et al., "Spread Spectrum Signaling for Speech Watermarking", United States Patents, Patent No. US 6,892,175 B1, May 10, 2005.
- [11] S. Erküçük, et. al., "A Robust Audio Watermark Representation Based on Linear Chirps", IEEE Transactions on Multimedia, Vol. 8, No. 5, October 2000
- [12] E. Ambikairajah, et. al., "Auditory masking and MPEG-1 audio", Electronics & Communication Engineering Journal, p165-175, August 1997
- [13] D. Torrieri, "Principles of Spread-Spectrum Communication Systems", Springer, p129-177, 2005
- [6] L. Boney, et. al., "Digital watermarks for audio signal", International Conf. on Multimedia Computing and Systems, Hiroshima, Japan, pp. 473-480, 1996
- [7] H. J. Kim, et. al., "A Novel Echo-Hiding Scheme With Backward and Forward Kernels", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 13, No. 8, August 2003.
- [8] B.S. Ko, et. al., "Time-Spread Echo Method for Digital Audio Watermarking", IEEE Transactions on Multimedia, Vol. 7, No. 2, April 2005.
- [9] P. Bassia, et. al., "Robust Audio Watermarking in the Time Domain", IEEE Transactions on Multimedia, Vol. 3, No. 2, June 2001.